Amendments to the Claims:

1. (Currently amended) A system for distributing digital documents having usage rights associated therewith, said system comprising:

a server having at least one digital document stored thereon;

a client computer having a standard application program including a rendering engine capable of being accessed to render content;

a communications network coupled to said client and said server; and

a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine,

wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content and thus grants or denies the request to access the content based on the usage rights associated with the content.

2. (Previously presented) A system as recited in claim 1, wherein the security conditions include the usage rights associated with the content.

3. (Original) A system as recited in claim 2, wherein the usage rights specify a manner of use of the content and conditions for exercising the manner of use.

4. (Original) A system as recited in claim 1, wherein said security module is operative to determine if said client computer is missing any security component software based on a predetermined configuration required for managing security of requested content and if said at least one client unit is missing any security component software based on said predetermined configuration, said security module is operative to provide said missing security component software to said client computer.

5. (Original) A system as recited in claim 1, wherein said security module is operative to check the content to determine if requested content requires a client side component of said security module and to disengage the client side security component from the standard application if the requested content does not require a client side security component.

6. (Original) A system as recited in claim 1, wherein said server comprises plural server computers and said security module is operative to cause said client computer to exchange one or more keys with a first of said server computers to obtain a validation certificate, said validation certificate permitting said client computer to securely communicate with a second of said server computers without any further exchange of keys between said client computer and any of said server computers.

7. (Original) A system as recited in claim 1, wherein said security module is operative to define a user interface of said standard application in accordance with parameters specified by said server.

8. (Original) A system as recited in claim 1, wherein parameters comprise specifications describing at least one of buttons, colors, patterns, animations, menus, and tool bars.

9. (Original) A system as recited in claim 1, wherein said security module is operative to superimpose a watermark based on client specific data on a image rendered by said rendering engine.

10. (Original) A system as recited in claim 9, wherein the client specific data is unique to the standard application.

11. (Original) A system as recited in claim 9, wherein the client specific data is unique to the client computer.

12. (Original) A system as recited in claim 1, further comprising a transaction aggregator system for managing transactions relating to document distribution and wherein said security module comprises a server side security component that directs the client computer to the transaction aggregator to receive a client side security component in exchange for transmitting user information to the transaction aggregator when said client computer makes a request for content and when said client side security component is not installed in said client computer, and wherein said transaction aggregator validates said client computer, based on predetermined conditions, and wherein said client side security component is unique to thereby identify said client computer to said server and to permit said server to report information relating to

transactions with said client side computer to said transaction aggregator.

13. (Original) A system as recited in claim 12, wherein said request is a request for purchase of digital content, and said one or more requirements are purchase price and a manner of use of said digital content.

14. (Original) A system as recited in claim 13, wherein said digital content comprises at least one of text, video, music, sound, and multimedia.

15. (Original) A system as recited in claim 9, wherein said information relating to transactions included purchase price information and wherein said transaction aggregator tracks and accumulates said purchase price information for each client computer for a predetermined period of time.

16. (Original) A system as recited in claim 15, wherein each transaction is a micro-transaction request which is accumulated by said content aggregator and the total value is transmitted to a credit card company at the end of each period.

17. (Original) A system as recited in claim 12, wherein said server does not obtain the user information of said client computer.

18. (Original) A system as recited in claim 1, wherein said server comprises a storage device containing a folder of embedded links to digital content and wherein the address of said folder is selected one of and to be difficult to ascertain, said security module being operative to provide information relating to at least one of the links when said client computer sends a request for content to said server and said security module indicates that that said client computer is authorized to access the content.

19. (Original) A system according to claim 18, wherein said digital content is a chapter of a book, and said request is a request for renting said chapter of said book for a predetermined period of time.

20. (Original) A system as recited in claim 1, wherein said security module creates a

document containing references to the digital content and spawns a child instance of the rendering engine to render the document, and wherein said child instance of said rendering engine is operative to follow the references to retrieve content through an asynchronous protocol from a secured location.

21. (Original) A system as recited in claim 20, wherein said secured location is a trusted server system.

22. (Original) A system as recited in claim 21, wherein said rendering engine is a Web browser.

23. (Original) A system as recited in claim 1, further comprising a trusted server system and wherein said security module is operative to check security information of executable code to be loaded on said client computer to ascertain if said executable code is certified for security and if said executable code is certified, permitting said executable code to be installed on said client computer and wherein if said executable code is not certified, said server contacts said trusted site to verify if said executable code is certified by said trusted site and permits said executable code to be installed on said client computer if said executable code is authorized.

24. (Original) A system as recited in claim 1, wherein said security module is operative to encrypt first portions of data transferred from said server to said client computer while second portions of said data are sent to said client computer without any encryption, and wherein the ratio of the size of said first portions of said data stream to the total size of said data stream is less than a predetermined maximum number and said ratio of the size of said first portions of said data to the total size of said data is selected based on communication variables monitored by said security component.

25. (Original) A system as recited in claim 24, wherein said communication variables comprise at least one of the total amount of data to be transferred, the communication network latency, and the communication speed.

26. (Original) A system as recited in claim 1, wherein said security module is operative to look for a signature on a request from said client computer to said server and if the signature

does not exist, to send a software agent from said server to said client computer, and wherein said software agent is operative to check said client computer to determine if said client computer is secured and the request is signed and returned to said server if said agent determines that said client computer is secured.

27. (Original) A system as recited in claim 26, wherein said request is a URL request.

28. (Original) A system as recited in claim 1, wherein said security component embeds all security information in a header of a document transmitted between said client computer and said server, said document having a body that does not contain security information for content in the document.

29. (Original) A system as recited in claim 28, wherein said document is an HTML document.

30. (Original) A system as recited in claim 1, wherein said security module is operative to check a request made by said client computer at two stages, a first stage filter checks if said request corresponds to a prohibited URL and a second stage filter checks if said request corresponds to a prohibited directory, and wherein if said request corresponds to a prohibited URL, or if said request corresponds to a prohibited directory, then said request is denied by said server.

31. (Original) A system as recited in claim 30, wherein if said request is denied by said server, said security module is operative to direct said client computer to present an appropriate access authorization before transferring content.

32. (Original) A system as recited in claim 1, wherein in response to a request for said of least one document, said security module is operative to package a file having a filename extension and being in a predetermined format, said filename extension being indicative of a format different from the predetermined format but compliant with said rendering engine, said file including references to a program suitable for rendering content contained in said file, said references being compliant with said rendering engine, said rendering engine being operative to open the file and follow the references to obtain and install the program to thereby render the

content.

33. (Original) A system as recited in claim 32, wherein said predetermined format is HTML.

34. (Original) A system as recited in claim 32, wherein said file contains content of a requested one of said documents.

35. (Original) A system as recited in claim 1, wherein said security module is operative to return a token to said client computer in response to a request sent from said client computer to said server, said token including a time stamp indicating a length of time that an authentication signature is valid.

36. (Original) A system as recited in claim 1, wherein said server comprises a plurality of related server computers.

37. (Currently amended) A method for distributing digital documents having usage rights associated therewith, said method comprising:

storing at least one digital document on a server;

requesting, over a communications network, the at least one digital document from a client computer having a standard application program including a rendering engine capable of being accessed to render content; and

enforcing security conditions for accessing the rendering engine with a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions,

wherein the security module intercepts requests to the rendering engine that would enact a violation of usage rights associated with the content and thus grants or denies the request to access the content based on the usage rights associated with the content.

38. (Previously presented) A method as recited in claim 37, wherein the security conditions include the usage rights associated with the content.

39. (Original) A method as recited in claim 38, wherein the usage rights specify a

manner of use of the content and conditions for exercising the manner of use.

40. (Original) A method as recited in claim 37, wherein said enforcing step comprises determining if said client computer is missing any security component software based on a predetermined configuration required for managing security of requested content and if said at least one client unit is missing any security component software based on said predetermined configuration, providing said missing security component software to said client computer.

41. (Original) A method as recited in claim 37, wherein said enforcing step comprises determining if requested content requires a client side component of said security module and disengaging the client side security component from the standard application if the requested content does not require a client side security component.

42. (Original) A method as recited in claim 37, wherein said server comprises plural server computers and said enforcing step comprises causing said client computer to exchange one or more keys with a first of said server computers to obtain a validation certificate, said validation certificate permitting said client computer to securely communicate with a second of said server computers without any further exchange of keys between said client computer and any of said server computers.

43. (Original) A method as recited in claim 37, wherein said enforcing step comprises defining a user interface of said standard application in accordance with parameters specified by said server.

44. (Original) A method as recited in claim 37, wherein parameters comprise specifications describing at least one of buttons, colors, patterns, animations, menus, and tool bars.

45. (Original) A method as recited in claim 37, wherein said enforcing step comprises creating a client specific watermark based on client specific data and superimposing the client specific watermark on a image rendered by said rendering engine.

46. (Original) A method as recited in claim 45, wherein the client specific data is unique

to the standard application.

47. (Original) A method as recited in claim 37, wherein the client specific data is unique to the client computer.

48. (Original) A method as recited in claim 37, wherein said enforcing step comprises directing the client, with a server side security component, to a transaction aggregator system for managing transactions relating to document distribution to receive a client side security component in exchange for transmitting user information to the transaction aggregator when said client computer makes a request for content and when said client side security component is not installed in said client computer, and validating said client computer with said transaction aggregator based on predetermined conditions, and wherein said client side security component is unique to thereby identify said client computer to said server and to permit said server to report information relating to transactions with said client side computer to said transaction aggregator.

49. (Original) A method as recited in claim 38, wherein said request is a request for purchase of digital content, and said one or more requirements are purchase price and a manner of use of said digital content.

50. (Original) A method as recited in claim 49, wherein said digital content comprises at least one of text, video, music, sound, and multimedia.

51. (Original) A method as recited in claim 48, wherein said information relating to transactions includes purchase price information and wherein said transaction aggregator tracks and accumulates said purchase price information for each client computer for a predetermined period of time.

52. (Original) A method as recited in claim 51, wherein each transaction is a micro-transaction request which is accumulated by said content aggregator and the total value is transmitted to a credit card company at the end of each period.

53. (Original) A method as recited in claim 48, wherein said server does not obtain the

user information of said client computer.

54. (Original) A method as recited in claim 37, further comprising storing a folder of embedded links to digital content on said server and wherein the address of said folder is selected one of and to be difficult to ascertain, and wherein said enforcing step comprises providing information relating to at least one of the links when said client computer sends a request for content to said server and said security module indicates that that said client computer is authorized to access the content.

55. (Original) A method according to claim 54, wherein said digital content is a chapter of a book, and said request is a request for renting said chapter of said book for a predetermined period of time.

56. (Original) A method as recited in claim 37, wherein said enforcing step comprises creating a document containing references to the digital content and spawning a child instance of the rendering engine to render the document, and retrieving content through an asynchronous protocol from a secured location with said child instance of said rendering engine by following the references to.

57. (Original) A method as recited in claim 56, wherein said secured location is a trusted server method.

58. (Original) A method as recited in claim 57, wherein said rendering engine is a Web browser.

59. (Original) A method as recited in claim 37, wherein said enforcing step comprises checking security information of executable code to be loaded on said client computer to ascertain if said executable code is certified for security and if said executable code is certified, permitting said executable code to be installed on said client computer and wherein if said executable code is not certified, contacting a trusted site to verify if said executable code is authorized by said trusted site and permitting said executable code to be installed on said client computer if said executable code is authorized.

60. (Original) A method as recited in claim 37, wherein said enforcing step comprises encrypting first portions of data transferred from said server to said client computer while second portions of said data are sent to said client computer without any encryption, and wherein the ratio of the size of said first portions of said data stream to the total size of said data stream is less than a predetermined maximum number and said ratio of the size of said first portions of said data to the total size of said data is selected based on communication variables monitored by said security component.

61. (Original) A method as recited in claim 60, wherein said communication variables comprise at least one of the total amount of data to be transferred, the communication network latency, and the communication speed.

62. (Original) A method as recited in claim 37, wherein said enforcing step comprises looking for a signature on a request from said client computer to said server and if the signature does not exist, sending a software agent from said server to said client computer, and wherein said software agent is operative to check said client computer to determine if said client computer is secured and the request is signed and returned to said server if said agent determines that said client computer is secured.

63. (Original) A method as recited in claim 62, wherein said request is a URL request.

64. (Original) A method as recited in claim 37, wherein said enforcing step comprises embedding all security information in a header of a document transmitted between said client computer and said server, said document having a body that does not contain security information for content in the document.

65. (Original) A method as recited in claim 64, wherein said document is an HTML document.

66. (Original) A method as recited in claim 37, wherein said enforcing step comprises a first checking step for determining if a request made by said client computer corresponds to a prohibited URL and a second checking step for determining if said request corresponds to a prohibited directory, and wherein if said request corresponds to a prohibited URL, or if said

request corresponds to a prohibited directory, instructing said server to deny said request.

67. (Original) A method as recited in claim 66, wherein said enforcing step further comprises directing said client computer to present an appropriate access authorization before transferring content if said request is denied by said server.

68. (Original) A method as recited in claim 37, wherein said enforcing step comprises packaging a file having a filename extension and being in a predetermined format, said filename extension being indicative of a format different from the predetermined format but compliant with said rendering engine, said file including references to a program suitable for rendering content contained in said file, said references being compliant with said rendering engine, and opening the file with the rendering engine and following the references to obtain and install the program to thereby render the content.

69. (Original) A method as recited in claim 68, wherein said predetermined format is HTML.

70. (Original) A method as recited in claim 68, wherein said file contains content of a requested one of said documents.

71. (Original) A method as recited in claim 70, wherein said enforcing step comprises returning a token to said client computer in response to a request sent from said client computer to said server, said token including a time stamp indicating a length of time that an authentication signature is valid.

72. (Original) A method as recited in claim 37, wherein said server comprises a plurality of related server computers.

73. (Currently amended) A system as recited in claim 1, further comprising:

[[An]] an HTML document adapted to be rendered by Web browser in a secure environment, said document comprising:

an HTML header defined between header tags;

an HTML body containing content; and

security information embedded in said header, said security information being associated with one or more usage rights for the content,

wherein the HTML header, the HTML body, and the security information are delivered to a client computing system, and

the client computing system interprets the security information and honors the usage rights while processing the HTML body and the HTML header.

74. (Currently amended) ~~An HTML document~~ The system as recited in claim 73, wherein said body does not contain security information for content in the document.

75. (Currently amended) ~~An HTML document~~ The system as recited in claim 74, wherein said security information is in the form of an attribute of said header.